IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Paul C. Kocher et al.
SERIAL NO.:	09/930,836
FILING DATE:	August 15, 2001
TITLE:	CRYPTOGRAPHIC COMPUTATION USING MASKING TO PREVENT DIFFERENTIAL POWER ANALYSIS AND OTHER ATTACKS
EXAMINER:	Darrow, Justin T.
GROUP ART UNIT:	**2132**
ATTY. DKT. NO.:	44424162-8724

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: Sept 10, 2004 By: _____
Michael C. Martensen, Reg. No. 46,901

MAIL STOP RCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

SIR:

Pursuant to the provisions of 37 CFR. 1.56 and 1.97-1.98, Applicants hereby cite the references listed on the accompanying substitute PTO-1449 without inferring or suggesting, but instead expressly disclaiming any inference or suggestion, that any more pertinent reference exists. The filing of the information disclosure statement shall not be construed as a representation that a search has been made (37 CFR §1.97(g)), or an admission that the

information cited is, or is considered to be, material to patentability. Applicants enclose herewith copies of the all cited references. All references are in the English language.

The Commissioner is authorized to charge any fees required in connection with the submission of this IDS to deposit account number 19-3140. This sheet is being submitted in duplicate.

Respectfully submitted,

Sept 10, 2004

Michael C. Martensen
Registration No. 46,901
Attorney under Rule 34(a)

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, IL 60606-1080
Tel.: (415) 882-0357

enclosures

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	AA	US-4,200,770	04/29/1980	Hellman et al.	
	AB	US-4,203,166	05/13/1980	Ehrsam et al.	
	AC	US-4,211,919	07/08/1980	Ugon	
	AD	US-4,214,126	07/22/1980	Wipff	
	AE	US-4,243,890	01/06/1981	Miller et al.	
	AF	US-4,405,829	09/20/1983	Rivest et al.	
	AG	US-4,759,063	07/19/1988	Chaum	
	AH	US-4,905,176	02/27/1990	Schulz	
	AI	US-5,136,643	08/04/1992	Fischer	
	AJ	US-5,241,598	08/31/1993	Raith	
	AK	US-5,297,201	03/22/1994	Dunlavy	
	AL	US-5,341,423	08/23/1994	Nossen	
	AM	US-5,369,706	11/29/1994	Latka	
	AN	US-5,404,402	04/04/1995	Sprunk	
	AO	US-5,412,379	05/02/1995	Waraska et al.	
	AP	US-5,539,827	07/23/1996	Liu	
	AQ	US-5,544,086	08/06/1996	Davis et al.	
	AR	US-5,546,463	08/13/1996	Caputo et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	AS	EP 0 529 261 A2	03/03/1993	IBM Corp.		☐
	AT	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp.		☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	AU	US-5,552,776	09/03/1996	Wade et al.	
	AV	US-5,559,887	09/24/1996	Davis et al.	
	AW	US-5,600,324	02/04/1997	Reed et al.	
	AX	US-5,633,930	05/27/1997	Davis et al.	
	AY	US-5,663,896	09/02/1997	Aucsmith	
	AZ	US-5,733,047	03/31/1998	Furuta et al.	
	BA	US-5,761,306	06/02/1998	Lewis	
	BB	US-5,778,065	07/07/1998	Hauser et al.	
	BC	US-5,848,159	12/08/1998	Collins et al.	
	BD	US-5,991,415	11/23/1999	Shamir	
	BE	US-5,995,629	11/30/1999	Reiner	
	BF	US-6,041,122	03/31/2000	Graunke et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (08-00)
Please type a plus sign (+) inside this box ™ +
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	BG	BELLARE et al., "Incremental Cryptography: The Case of Hashing and Signing" in: DESMEDT, Y., Advances in Cryptology - Crypto '96 (Berlin, Springer, 1996), pp. 104-113	
	BH	MENZES et al., "Handbook of Applied Cryptography" (CRC Press, 1996), pages including 285-298, 312-319, 452-462, 475, 512-524	
	BI	Bank Technology News. "Cries of Wolf Over Smart Card Security?" Faulkner & Gray, Inc. 01 November 1996	
	BJ	American National Standards for Financial Services, secretariat - American Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key Management," approved April 6, 1992, American National Standards Institute; pgs. 1-71	
	BK	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127	
	BL	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical University Munich, 1998; pgs. 31-48	
	BM	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure Your Wireless Designs", 01/18/96; pgs. 57-68	
	BN	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt 91, 1991; pgs. 453-460	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Please type a plus sign (+) inside this box ™ [+]

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Darrow, Justin T.
Attorney Docket Number	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	BO	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994, Chapter III; pgs. 53-77	
	BP	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91, 1991; pgs. 17-38	
	BQ	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful Adversary?" 1999	
	BR	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6	
	BS	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories, Bulletin, Number 2, January 23, 1996	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.